

# Flags of almost affine codes

Trygve Johnsen\*

Hugues Verdure†

April 11, 2017

## Abstract

We describe a two-party wire-tap channel of type II in the framework of almost affine codes. Its cryptological performance is related to some relative profiles of a pair of almost affine codes. These profiles are analogues of relative generalized Hamming weights in the linear case.

Keywords: two-party wire-tap channel of type II, almost affine codes

## 1 Introduction

In [8], Ozarow and Wyner describe the wire-tap channel of type II. The idea is to encrypt a message  $\mathbf{m}$  without the use of any key (public or private), and send the encrypted message on a noiseless channel. The intruder is able to listen to parts of the encrypted message. One is interested in designing a system that gives as little information as possible to the intruder. In their original paper, the authors give a system using linear codes: given a  $(n, n - k)$  parity check matrix  $H$  of the linear code, the sender picks up uniformly and at random a preimage by  $H$  of  $\mathbf{m}$ , where  $\mathbf{m}$  is seen as a column vector of length  $n - k$ , and sends this preimage of length  $n$  over the channel.

In [10], Wei relates the maximum amount of information collected by the intruder to the generalized Hamming weights of the dual of the linear code.

In [6], the authors look at a variant of Ozarow and Wyner's scheme, namely the so-called two-party wire-tap channel of type II. This time, the intruder, not only is able to listen to parts of the encrypted message, but also knows a part of the original message. This leads to the study of pairs of linear codes. In [5] and [11], the authors look at relative generalized Hamming weights and relative dimension/length profiles of such pairs of codes, and they relate these quantities to the amount of information gathered by the intruder in the two-party wire-tap channel of type II.

Almost affine codes are a strict generalization of linear/affine codes, introduced by Simonis and Ashikhmin in [9]. In [4], we give a scheme for the wire-tap channel of type II that uses almost affine codes. We also give an analogue of Wei's result relating the amount of information gained by the intruder to the generalized Hamming weights of the dual of the matroid associated to the almost affine code.

In the present paper, we look at the two-party wire-tap channel of type II for almost affine codes. We build on the scheme presented in [4]. As in [6], the intruder is now allowed to listen to parts of the encrypted message and knows parts of the original message. We build a larger almost affine code that only depends on the part of the original message known to the intruder. At this point, we deviate from the scheme in [6], where the subset of the original symbols tapped by the intruder, as described in that paper, corresponds to a (linear) subcode, say  $C_2$ , of  $C$ . Hence our scheme, specialized to the subclass of linear codes, is not exactly the same as that of [6]. If, however, in [6],

---

\*Dept. of Mathematics, UiT The Arctic University of Norway, N-9037 Tromsø, Norway, [Trygve.Johnsen@uit.no](mailto:Trygve.Johnsen@uit.no)

†Dept. of Mathematics, UiT The Arctic University of Norway, N-9037 Tromsø, Norway, [Hugues.Verdure@uit.no](mailto:Hugues.Verdure@uit.no)

one simply chooses to look at the dualized codes, one gets a set-up, which is closer to ours, since the tapped symbols of the original message then correspond to a larger code  $C_2^*$  containing  $C^*$ . Thus our scheme is an analogue of the one in [6].

A unifying theme for all four set-ups (the ones in [10], [6], [4], and the present one) is that of rank functions. Each linear or almost affine code defines a rank function of a matroid. Moreover each pair of a code and a subcode comes equipped by a rank function  $\rho$ , which is the difference of the two (matroid) rank function of the codes in question. The function  $\rho$  is not necessarily a matroid rank function, but it is a so-called demi-matroid rank function. Demi-matroids were defined and described in [2], and so-called profiles of demi-matroids were further described in [1]. The relative Hamming weights of pairs of linear codes, as described in [6], are examples of such profiles. We analyze the performance of our cryptological set-up, and find that it is described in detail by an essential profile of the associated demi-matroid. This is formulated in our main result, Theorem 5.

The paper is organized as follows: in Section 2, we recall basic definitions and properties about matroids, demi-matroids and almost affine codes.

In Section 3, we study flags, or chains, of almost affine codes, and the demi-matroids formed by the alternating sums of their rank functions. A main result is Proposition 4, which is a generalization of [1, Theorem 9]. Flags of length two will be of particular interest in remaining part of the paper.

In Section 4 we investigate a two-party wire tap channel of type II, and describe in detail how we use an almost affine code  $C$  and a certain function  $\varphi : A \times A \rightarrow A$  for the code alphabet  $A$ , to encode messages. Moreover we describe another bigger almost affine code  $D$  that corresponds to uncoded symbols tapped by an adversary. By means of an entropy analysis we arrive at our conclusions. We also give an example with a non-linear almost affine code, whose associated matroid is the non-Pappus matroid of length 9 and rank 3.

## 2 Matroids, demi-matroids and almost affine codes

In this section, we essentially recall relevant material that will be needed in the sequel, and we do not claim to have any new results here. We refer to [7] for the theory of matroids, to [2] for an introduction on demi-matroids and to [9] for an introduction on almost affine codes, and we will use their notation.

### 2.1 Matroids and demi-matroids

A matroid is a combinatorial structure that extend the notion of linear (in)dependency. There are many equivalent definitions, but we will give just one here.

**Definition 1** *A matroid is a pair  $M = (E, r)$  where  $E$  is a finite set, and  $r$  a function on the power set of  $E$  into  $\mathbb{N}$  satisfying the following axioms:*

- (R1)  $r(\emptyset) = 0$ ,
- (R2) for every subset  $X \subset E$  and  $x \in E$ ,  $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$ ,
- (R3) for every  $X \subset E$  and  $x, y \in E$ , if  $r(X) = r(X \cup \{x\}) = r(X \cup \{y\})$ , then  $r(X \cup \{x, y\}) = r(X)$ .

The set  $E$  is called the ground set, and the function  $r$  the rank function. Any subset  $X \subset E$  with  $r(X) = |X|$  is called independent. A basis is a inclusion maximal independent set. Finally, the rank  $r(M)$  of the matroid  $M$  is  $r(E)$ , and is also the cardinality of any basis.

Demi-matroids were introduced in [2] and elaborated on in [1] when the authors studied flags of linear codes. They are a generalization of matroids in the following way:

**Definition 2** A demi-matroid is a pair  $M = (E, r)$  where  $E$  is a finite set, and  $r$  a function on the power set of  $E$  into  $\mathbb{N}$  satisfying axioms (R1) and (R2) above.

**Remark 1** The definitions in [2, 1] are different, but equivalent. See for example [3, Theorem 5.5]

As for matroids, the set  $E$  is called the ground set, and the function  $r$  the rank function. The rank  $r(M)$  of the demi-matroid  $M$  is  $r(E)$ .

Matroids and demi-matroids have duals defined in the following way:

**Proposition 1** Let  $M = (E, r)$  be a matroid (respectively a demi-matroid). Then  $M^* = (E, r^*)$  with  $r^*$  defined as

$$r^*(X) = |X| + r(E \setminus X) - r(E)$$

is a matroid (respectively a demi-matroid). Moreover,  $(M^*)^* = M$ .

**Proof** The fact that  $r^*$  is the rank function of a matroid if  $r$  is so, is contained in any standard textbook on matroids, e.g. [7]. The fact that  $r^*$  is the rank function of a demi-matroid if  $r$  is so, is immediate from axioms (R1) and (R2). ■

The matroid (respectively demi-matroid)  $M^*$  is called the dual (respectively the dual or first dual) of  $M$ . It has rank  $|E| - r(M)$ . Demi-matroids have another dual, called the supplement dual or second dual:

**Proposition 2** Let  $M = (E, r)$  be a demi-matroid. Then  $\overline{M} = (E, \bar{r})$  with  $\bar{r}$  defined as

$$\bar{r}(X) = r(E) - r(E \setminus X)$$

is a demi-matroid. Moreover, we have  $\overline{\overline{M}} = M$  and  $\overline{M^*} = \overline{M}^*$ .

**Proof** See [2, Theorem 4]. ■

## 2.2 Almost affine codes

Almost affine codes were first introduced in [9], and are a combinatorial generalization of affine codes.

**Definition 3** An almost affine code on a finite alphabet  $A$ , of length  $n$  and dimension  $k$  is a subset  $C \subset A^n$  such that  $|C| = |A|^k$  and such that for every subset  $X \subset E = \{1, \dots, n\}$ ,

$$\log_{|A|} |C_X| \in \mathbb{N},$$

where  $C_X$  is the puncturing of  $C$  with respect to  $E \setminus X$ .

An almost affine subcode of  $C$  is a subset  $D \subset C$  which is itself an almost affine code on the same alphabet.

**Remark 2** Any linear or affine code is obviously an almost affine code.

To any almost affine code  $C$  of length  $n$  and dimension  $k$  on the alphabet  $A$ , we can associate a matroid  $M_C$  on the ground set  $E = \{1, \dots, n\}$  and with rank function

$$r(X) = \log_{|A|} |C_X|,$$

for  $X \subset E$ .

**Example 1** Consider the almost affine code  $C'$  in [9, Example 5]. It is a code of length 3 and dimension 2 on the alphabet  $A = \{0, 1, 2, 3\}$ . Its set of codewords is

000	011	022	033
101	112	123	130
202	213	220	231
303	310	321	332

Its matroid is the uniform matroid  $U_{2,3}$  of rank 2 on 3 elements. This is an example of an almost affine code which is not equivalent to a linear code.

While it is easy to see that any linear code has subcodes of a given dimension (and we even know the number of such subcodes), it is not straightforward to do so for almost affine codes. This is what we summarize here now.

**Definition 4** Let  $C$  be a block code of length  $n$ , and let  $\mathbf{c} \in C$  be fixed. The  $\mathbf{c}$ -support of any codeword  $\mathbf{w}$  is

$$\text{Supp}(\mathbf{w}, \mathbf{c}) = \{i, \mathbf{c}_i \neq \mathbf{w}_i\}.$$

The  $\mathbf{c}$ -support of  $C$  is

$$\text{Supp}(C, \mathbf{c}) = \bigcup_{\mathbf{w} \in C} \text{Supp}(\mathbf{w}, \mathbf{c}).$$

Note that the  $\mathbf{c}$ -support of the code is independent of the choice of  $\mathbf{c} \in C$  (see [4, Lemma 1]), and it will therefore be denoted by  $\text{Supp}(C)$  without reference to any codeword.

**Definition 5** Let  $C$  be an almost affine code of length  $n$ , and let  $\mathbf{c} \in F^n$  be fixed. Then

$$C(X, \mathbf{c}) = \{\mathbf{w} \in C, \mathbf{w}_X = \mathbf{c}_X\},$$

where  $\mathbf{w}_X$  is the projection of  $\mathbf{w}$  to  $X$ .

This might be empty, or not be an almost affine code, but when we take  $\mathbf{c} \in C$ , we get the following ([9, Corollary 1]):

**Proposition 3** Let  $C$  be an almost affine code of length  $n$  and dimension  $k$  on the alphabet  $A$ . Let  $\mathbf{c} \in C$ . Let  $X \subset \{1, \dots, n\}$ . Then  $C(X, \mathbf{c})$  is an almost affine subcode of  $C$ , and moreover, the rank function  $\rho$  of the matroid associated to  $C(X, \mathbf{c})$  is given by

$$\rho(Y) = r(X \cup Y) - r(X)$$

where  $r$  is the rank function of the matroid  $M_C$ . In particular,

$$|C(X, \mathbf{c})| = |A|^{k-r(X)}.$$

**Corollary 1** Every almost affine code  $C$  of dimension  $k$  has almost affine subcodes of dimension  $0 \leq i \leq k$ .

### 3 Flags of demi-matroids and almost affine codes

In this section, we look at flags of (demi-)matroids and almost affine codes. We show that under certain assumptions, they give rise to a demi-matroid in a natural way. These assumptions are always satisfied for flags of almost affine codes. We are mainly interested in pairs of codes in the next section, but for the sake of generality, we look at flags.

### 3.1 Flags of demi-matroids

**Definition 6** A flag of demi-matroids is a finite set of demi-matroids  $M_i = (E_i, r_i)$  for  $1 \leq i \leq m$  on the same ground set  $E$ , and such that

$$\forall X \subset E, r_m(X) \leq \dots \leq r_2(X) \leq r_1(X).$$

A pair of demi-matroids is a flag with two demi-matroids.

Given a flag of demi-matroids as above, we can define a function  $\rho$  on the power set of  $E$  as the alternative sum of the rank functions, namely

$$\forall X \subset E, \rho(X) = \sum_{i=1}^m (-1)^{i+1} r_i(X).$$

It is natural to ask when the pair  $M = (E, \rho)$  is a demi-matroid.

**Definition 7** Let  $M = (E, r)$  be a demi-matroid. Let

$$\mathcal{E}_M = \{(X, x), X \subset E, x \in X, r(X \setminus \{x\}) = r(X)\}.$$

**Theorem 1** Let  $(M_1, M_2)$  be a pair of demi-matroids on the ground set  $E$ . Then  $(E, \rho)$ , where  $\rho$  is defined above, is a demi-matroid if and only if  $\mathcal{E}_{M_1} \subset \mathcal{E}_{M_2}$ .

**Proof** Suppose first that  $(E, \rho)$  is a demi-matroid. Then, for every  $X \subset E$  and any  $x \in X$ , we have

$$\rho(X \setminus \{x\}) \leq \rho(X).$$

Assume that  $(X, x) \in \mathcal{E}_{M_1}$ . Then

$$\begin{aligned} r_2(X) - r_2(X \setminus \{x\}) &= r_1(X) - \rho(X) - r_1(X \setminus \{x\}) + \rho(X \setminus \{x\}) \\ &= r_1(X) - r_1(X \setminus \{x\}) - (\rho(X) - \rho(X \setminus \{x\})) \\ &= 0 - (\rho(X) - \rho(X \setminus \{x\})) \\ &\leq 0. \end{aligned}$$

But we also have

$$r_2(X) - r_2(X \setminus \{x\}) \geq 0$$

which proves that this is in  $\mathcal{E}_{M_2}$  too.

Assume now that  $\mathcal{E}_{M_1} \subset \mathcal{E}_{M_2}$ . (R1) is trivially fulfilled by  $\rho$ . And let  $X \subset E$ ,  $x \in E$ . We compute

$$\begin{aligned} \rho(X \cup \{x\}) - \rho(X) &= r_1(X \cup \{x\}) - r_2(X \cup \{x\}) - (r_1(X) - r_2(X)) \\ &= (r_1(X \cup \{x\}) - r_1(X)) - (r_2(X \cup \{x\}) - r_2(X)) \end{aligned}$$

We have 3 cases

- If  $(X \cup \{x\}, x) \in \mathcal{E}_{M_1} \subset \mathcal{E}_{M_2}$ , then

$$\rho(X \cup \{x\}) - \rho(X) = (r_1(X \cup \{x\}) - r_1(X)) - (r_2(X \cup \{x\}) - r_2(X)) = 0 - 0 = 0,$$

- If  $(X \cup \{x\}, x) \in \mathcal{E}_{M_2} \setminus \mathcal{E}_{M_1}$ , then

$$\rho(X \cup \{x\}) - \rho(X) = (r_1(X \cup \{x\}) - r_1(X)) - (r_2(X \cup \{x\}) - r_2(X)) = 1 - 0 = 1,$$

- If  $(X \cup \{x\}, x) \notin \mathcal{E}_{M_2}$ , then

$$\rho(X \cup \{x\}) - \rho(X) = (r_1(X \cup \{x\}) - r_1(X)) - (r_2(X \cup \{x\}) - r_2(X)) = 1 - 1 = 0.$$

In any cases,

$$\rho(X) \leq \rho(X \cup \{x\}) \leq \rho(X) + 1.$$

■

We can now generalize to flags of demi-matroids. Note that this generalization is just an implication, not an equivalence.

**Theorem 2** *Let  $(M_1, \dots, M_m)$  be a flag of matroids. If  $\mathcal{E}_{M_1} \subset \mathcal{E}_{M_2} \subset \dots \subset \mathcal{E}_{M_m}$ , then  $(E, \rho)$  with  $\rho$  defined above is a demi-matroid.*

**Proof** For simplicity, we write  $\mathcal{E}_j$  for  $\mathcal{E}_{M_j}$ . The fact that  $\rho(\emptyset) = 0$  is trivial. Now, let  $X \subset E$  and  $x \in E$ . Let  $j$  be minimal such that  $(X \cup \{x\}, x) \in \mathcal{E}_j \setminus \mathcal{E}_{j-1}$  with the convention that  $j = 1$  if  $(X \cup \{x\}, x) \in \mathcal{E}_1$  and  $j = m + 1$  if  $(X \cup \{x\}, x) \notin \mathcal{E}_m$ . Then we have

$$\begin{aligned} \rho(X \cup \{x\}) &= \sum_{i=1}^m (-1)^{i+1} r_i(X \cup \{x\}) \\ &= \sum_{i=1}^{j-1} (-1)^{i+1} r_i(X \cup \{x\}) + \sum_{i=j}^m (-1)^{i+1} r_i(X \cup \{x\}) \\ &= \sum_{i=1}^{j-1} (-1)^{i+1} [r_i(X) + 1] + \sum_{i=j}^m (-1)^{i+1} r_i(X) \\ &= \rho(X) + \sum_{i=1}^{j-1} (-1)^{i+1} \end{aligned}$$

Independently on the parity of  $j$ , we always have

$$0 \leq \rho(X \cup \{x\}) - \rho(X) \leq 1.$$

■

### 3.2 Flags of almost affine codes

**Definition 8** *A flag  $F = (C_1, \dots, C_m)$  of almost affine codes is a finite set of almost affine codes on the same alphabet and same length, with the property that for  $1 \leq j \leq m - 1$ ,  $C_{j+1}$  is an almost affine subcode of  $C_j$ . A pair of almost affine codes is a flag with two codes.*

We will see in this section that flags of almost affine codes give rise to demi-matroids in a natural way. We will also look at the duals of these demi-matroids. We start with a lemma.

**Lemma 1** *Let  $C$  be an almost affine code,  $\mathbf{w} \in C$ . Let  $X \subset E$  and  $x \in E \setminus X$ . Then*

$$r(X \cup \{x\}) = r(X) \Leftrightarrow C(X \cup \{x\}, \mathbf{w}) = C(X, \mathbf{w}).$$

**Proof** We always have  $C(X \cup \{x\}, \mathbf{w}) \subset C(X, \mathbf{w})$ . Then it is a direct consequence of Proposition 3.

■

**Lemma 2** Let  $(C_1, C_2)$  be a pair of almost affine codes. Let  $\mathbf{w} \in C_2$ , and  $X \subset E$ . Then

$$C_2(X, \mathbf{w}) = C_2 \cap C_1(X, \mathbf{w}).$$

**Proof** This is obvious.  $\blacksquare$

Given a flag of almost affine codes  $F = (C_1, \dots, C_m)$  of length  $n$ , define the following function on the power set of  $E = \{1, \dots, n\}$  by

$$\rho_F(X) = \sum_{i=1}^m (-1)^{i+1} r_i(X)$$

for  $X \subset E$ , where  $r_i$  is the rank function of the matroid associated to  $C_i$ .

**Theorem 3** Let  $F = (C_1, \dots, C_m)$  be a flag of almost affine codes. Then the pair  $(E, \rho_F)$  defined above is a demi-matroid.

**Proof** As before, we write  $\mathcal{E}_j$  instead of  $\mathcal{E}_{M_j}$ , where  $M_j$  is the matroid associated to  $C_j$ . By Theorem 2, it suffices to show that  $\mathcal{E}_j \subset \mathcal{E}_{j+1}$ , for  $1 \leq j \leq m-1$ . Let  $(X, x) \in \mathcal{E}_j$  and  $\mathbf{w} \in C_{j+1} \subset C_j$ . From Lemma 1, this means that

$$C_j(X \setminus \{x\}, \mathbf{w}) = C_j(X, \mathbf{w}).$$

Then by Lemma 2,

$$C_{j+1}(X \setminus \{x\}, \mathbf{w}) = C_{j+1}(X, \mathbf{w}),$$

and by Lemma 1 again,  $(X, x) \in \mathcal{E}_{j+1}$ .  $\blacksquare$

Almost affine codes generally do not have duals. Their associated (demi-)matroids have, and we could have defined functions using  $r_i^*$ ,  $\overline{r}_i$  or  $\overline{r}_i^*$ . In the sequel we see what are the relations between these alternative functions.

**Lemma 3** Let  $M_1 = (E, r_1)$  and  $M_2 = (E, r_2)$  be two demi-matroids. Then

$$\mathcal{E}_{M_1} \subset \mathcal{E}_{M_2} \Leftrightarrow \mathcal{E}_{M_2^*} \subset \mathcal{E}_{M_1^*} \Leftrightarrow \mathcal{E}_{\overline{M_1}} \subset \mathcal{E}_{\overline{M_2}}.$$

**Proof** Suppose that  $\mathcal{E}_{M_1} \subset \mathcal{E}_{M_2}$ . Let  $(X, x) \in \mathcal{E}_{M_2^*}$ . Then

$$|X \setminus \{x\}| + r_2(E \setminus (X \setminus \{x\})) - r_2(E) = |X| + r_2(E \setminus X) - r_2(E),$$

that is

$$r_2(E \setminus X) = r_2((E \setminus X) \cup \{x\}) - 1.$$

In other words,  $((E \setminus X) \cup \{x\}) \notin \mathcal{E}_{M_2}$  and consequently  $((E \setminus X) \cup \{x\}) \notin \mathcal{E}_{M_1}$  either, that is

$$r_1(E \setminus X) = r_1((E \setminus X) \cup \{x\}) - 1$$

by the definition of  $\mathcal{E}_{M_1}$  and (R2). Then

$$\begin{aligned} r_1^*(X \setminus \{x\}) &= |X \setminus \{x\}| + r_1(E \setminus (X \setminus \{x\})) - r_1(E) \\ &= |X| - 1 + r_1(E \setminus X) + 1 - r_1(E) \\ &= r_1^*(X), \end{aligned}$$

that is  $(X, x) \in \mathcal{E}_{M_1^*}$ . Let now  $(X, x) \in \mathcal{E}_{\overline{M_1}}$ , that is

$$r_1(E) - r_1(E \setminus (X \setminus \{x\})) = \overline{r}_1(X \setminus \{x\}) = \overline{r}_1(X) = r_1(E) - r_1(E \setminus X).$$

Then  $((E \setminus X) \cup \{x\}, x) \in \mathcal{E}_{M_1} \subset \mathcal{E}_{M_2}$ , and by the same computation for  $\overline{r}_2$ ,  $(X, x) \in \mathcal{E}_{\overline{M_2}}$ .

The two other implications follow by duality.  $\blacksquare$

**Proposition 4** Let  $F = (C_1, \dots, C_m)$  be a flag of almost affine codes, with  $r_i$  be the rank function of the matroid associated to the code  $C_i$  for  $1 \leq i \leq m$ . Define the following functions:

$$\begin{aligned}\eta_F &= \sum_{i=1}^m (-1)^{m-i} r_i^*, \\ \theta_F &= \sum_{i=1}^m (-1)^{i+1} \overline{r_i}, \\ \pi_F &= \sum_{i=1}^m (-1)^{m-i} \overline{r_i^*}.\end{aligned}$$

Then  $(E, \eta_F)$ ,  $(E, \theta_F)$  and  $(E, \pi_F)$  are all demi-matroids. Moreover, we have the following duality relations:

$$\eta_F = \begin{cases} \overline{\rho_F} & \text{if } m \text{ is even} \\ \rho_F^* & \text{if } m \text{ is odd} \end{cases}, \quad \theta_F = \overline{\rho_F}, \quad \pi_F = \begin{cases} \rho_F & \text{if } m \text{ is even} \\ \overline{\rho_F^*} & \text{if } m \text{ is odd} \end{cases}.$$

**Proof** The first part of the proposition is an easy adaptation of the proof of the previous theorem, together with the previous lemma. For the second part, we compute

$$\begin{aligned}\eta_F(X) &= \sum_{i=1}^m (-1)^{m-i} r_i^*(X) \\ &= \sum_{i=1}^m (-1)^{m-i} [|X| + r_i(E \setminus X) - r_i(E)] \\ &= \sum_{i=1}^m (-1)^{m-i} |X| + \sum_{i=1}^m (-1)^{m-i} r_i(E \setminus X) - \sum_{i=1}^m (-1)^{m-i} r_i(E) \\ &= \begin{cases} 0 - \sum_{i=1}^m (-1)^{i+1} r_i(E \setminus X) + \sum_{i=1}^m (-1)^{i+1} r_i(E) & \text{if } m \text{ is even} \\ |X| + \sum_{i=1}^m (-1)^{i+1} r_i(E \setminus X) - \sum_{i=1}^m (-1)^{i+1} r_i(E) & \text{if } m \text{ is odd} \end{cases} \\ &= \begin{cases} \overline{\rho_F} & \text{if } m \text{ is even} \\ \rho_F^* & \text{if } m \text{ is odd} \end{cases}\end{aligned}$$

The other equalities are done in a similar way. ■

**Remark 3** The corollary generalizes [1, Theorem 9], where the corresponding result was proven for flags of linear codes. In Part (b) the  $r_i^*$  are rank functions of the dual codes (orthogonal complements)  $C_i^\perp$  if the  $C_i$  are linear (or even multilinear) codes. If we only know that the  $C_i$  are almost affine, we do not necessarily have dual codes, for which the  $r_i^*$  are rank functions. See [4]. In Section 4, where we give the results and applications that we hope are the most interesting ones, it is only the case  $m = 2$  that is considered. The case of longer flags ( $m \geq 3$ ) was included above for completeness, and for possible usage in new, e.g. cryptological, applications that might turn up in the future (although we unfortunately have not found applications for chains of length 3 or more yet).

## 4 Two-party wire tap channel of type II

In [8], Ozarow and Wyner introduce the wire-tap channel of type II. The idea is to encode a message without the use of any key and send it over a channel where an intruder can listen to a subset of the transmitted symbols. The goal of the encoder is to minimize the information about the original



message the intruder can get. The authors propose a scheme using linear codes. In [10], the amount of information collected by the intruder is related to the generalized Hamming weights of the dual of the linear code. In [4], we give a scheme that uses almost affine codes, and give an analogue of Wei's result.

In [6], the authors look at the following two-party wiretap channel of type II: this time, the intruder is able to get some symbols of the original message, as well as to listen to a subset of the transmitted symbols. In this section, we investigate the same scenario for our scheme.

#### 4.1 Wiretap channel of type II for almost affine codes

We start by recalling our scheme described in [4]: let  $C$  be an almost affine code of length  $n$  and rank  $k$  on the alphabet  $A$ . Let  $B \subset E = \{1, \dots, n\}$  be a basis of the matroid  $M_C$ . Let  $\varphi : A \times A \rightarrow A$  be a function such that for every  $y \in A$ ,  $\varphi_{y,1} = \varphi(y, -)$  and  $\varphi_{y,2} = \varphi(-, y)$  are bijections. For  $\mathbf{m} \in A^{E \setminus B}$ , let  $\Phi_{\mathbf{m}} : A^E \rightarrow A^E$  be defined the following way: if  $\mathbf{w} \in A^E$ , then

$$\Phi_{\mathbf{m}}(\mathbf{w})_i = \begin{cases} \mathbf{w}_i & \text{if } i \in B \\ \varphi(\mathbf{w}_i, \mathbf{m}_i) & \text{if } i \in E \setminus B \end{cases}$$

We can then define, for  $\mathbf{m} \in A^{E \setminus B}$ ,

$$C_{\varphi, \mathbf{m}} = \Phi_{\mathbf{m}}(C).$$

Whenever  $\varphi$  is obvious from the context, we may omit it and write  $C_{\mathbf{m}}$  for  $C_{\varphi, \mathbf{m}}$ . From [4], we have the following:

**Lemma 4** *For every  $\mathbf{m} \in A^{E \setminus B}$ ,  $C_{\mathbf{m}}$  is an almost affine code of length  $n$  and dimension  $k$  over  $A$ , with associated matroid equal to  $M_C$ . Moreover, the codes  $C_{\mathbf{m}}$  for  $\mathbf{m} \in A^{E \setminus B}$  form a partition of  $A^E$ .*

The scheme is the following: one wishes to send the message  $\mathbf{m}$  over a channel. The sender chooses uniformly and at random an element  $\mathbf{w} \in C_{\mathbf{m}}$ . The receiver finds the unique  $\mathbf{m}'$  such that  $\mathbf{w} \in C_{\mathbf{m}'}$ . Then  $\mathbf{m}' = \mathbf{m}$ .

In [4], an intruder was able to listen to up to  $\mu$  of the  $n$  symbols sent over the channel. Then it is shown that whenever the intruder is able to listen up to  $d_{j+1}^*$  symbols of the transmitted message, then he has knowledge of at most  $j$  symbols of the original message, where  $d_j^*$  are the generalized Hamming weights of  $M_C^*$ .

#### 4.2 Two-party wiretap channel of type II for almost affine codes

In the two-party wiretap channel of type II, the intruder is able to get a subset  $X \subset E \setminus B$  of the original message  $\mathbf{m}$ , and to tap a subset  $Y \subset E$  of cardinality  $\mu$  of the transmitted message over the channel. We will now look into the equivocation of the system, that is the maximum of information gained by the intruder after these taps.

##### 4.2.1 An almost affine overcode

Let  $\mathbf{M} \in A^X$ . Define

$$D_{X, \mathbf{M}} = \bigcup_{\substack{\mathbf{m} \in A^{E \setminus B} \\ \mathbf{m}_X = \mathbf{M}}} C_{\mathbf{m}}.$$

**Lemma 5** For every  $X \subset E \setminus B$  and every  $\mathbf{M} \in A^X$ ,  $D_{X,\mathbf{M}}$  is an almost affine code of length  $n$  and rank  $n - |X|$  on  $A$ . Its associated matroid  $M_D$  has rank function

$$r_{D_{X,\mathbf{M}}}(Y) = |Y \setminus (B \cup X)| + r(Y \cap (B \cup X)).$$

It is independent of  $\mathbf{M}$ .

**Proof** For simplicity, we write  $D$  for  $D_{X,\mathbf{M}}$ . Let  $Y \subset E$ . We have to show that  $|D_Y|$  is a power of  $|A|$ . We define the following sets:

- $Y_1 = Y \cap (X \cup B)$ ,
- $Y_2 = Y \setminus Y_1$ ,
- $I \subset Y_1$  a maximal independent set of  $Y_1$  for the matroid associated to  $C$  (and therefore all  $C_{\mathbf{m}}$ ). Since  $B$  is a basis of the matroid, we may even assume that  $Y_1 \cap B \subset I$ .
- $J = Y_1 \setminus I$ ,
- $I_B = B \cap I = B \cap Y$ ,
- $I_X = X \cap I = I \setminus I_B$ .

The idea is to show that on one hand we have full freedom on the choice of the characters on  $Y_2$  and  $I$  for the words of  $D_Y$ , the first one because of the choice of  $\mathbf{m}$ , the second one because  $I$  is an independent set, which shows that we have  $|D_Y| \geq |A|^{|Y_2 \cup I|}$ . On the other hand, we show that if two words of  $D_Y$  agree on  $Y_2 \cup I$ , then they must agree on the rest of  $Y$  as well.

So let  $\mathbf{a} = (a_i)_{i \in Y_2 \cup I} \in A^{Y_2 \cup I}$ . Let  $\mathbf{b} = (b_j)_{j \in I} \in A^I$  defined by

$$b_j = \begin{cases} a_j & \text{if } j \in I_B \\ \varphi_{\mathbf{M}_j,2}^{-1}(a_j) & \text{if } j \in I_X \end{cases}$$

Since  $I$  is an independent set for the matroid  $M_C$ , there exists a word  $\mathbf{c} = (c_j)_{j \in E} \in C$  with

$$\mathbf{c}_I = \mathbf{b}.$$

Now, define  $\mathbf{m} = (m_i)_{i \in E \setminus B}$  in the following way :

$$m_i = \begin{cases} \mathbf{M}_i & \text{if } i \in X \\ \varphi_{c_i,1}^{-1}(a_i) & \text{if } i \in Y_2 \\ \text{randomly} & \text{otherwise} \end{cases}$$

Of course,  $\mathbf{m}_X = \mathbf{M}$ . Finally, look at the word  $\mathbf{w} = \Phi_{\mathbf{m}}(\mathbf{c})$ . Then, by construction,  $\mathbf{w} \in C_{\mathbf{m}} \subset D$  and  $\mathbf{w}_{I \cup Y_2} = \mathbf{a}$ .

Now, let  $\mathbf{w}_1, \mathbf{w}_2 \in D$  such that  $(\mathbf{w}_1)_{I \cup Y_2} = (\mathbf{w}_2)_{I \cup Y_2}$ . By definition, there exists  $\mathbf{c}_1, \mathbf{c}_2 \in C$  and  $\mathbf{m}_1, \mathbf{m}_2 \in A^{E \setminus B}$  with  $(\mathbf{m}_1)_X = (\mathbf{m}_2)_X = \mathbf{M}$  such that  $\mathbf{w}_1 = \Phi_{\mathbf{m}_1}(\mathbf{c}_1)$  and  $\mathbf{w}_2 = \Phi_{\mathbf{m}_2}(\mathbf{c}_2)$ .

In particular, we have that

$$(\mathbf{c}_1)_{I_B} = (\Phi_{\mathbf{m}_1}(\mathbf{c}_1))_{I_B} = (\mathbf{w}_1)_{I_B} = (\mathbf{w}_2)_{I_B} = (\Phi_{\mathbf{m}_2}(\mathbf{c}_2))_{I_B} = (\mathbf{c}_2)_{I_B}$$

and for every  $i \in I_X$ ,

$$\varphi((\mathbf{c}_1)_i, (\mathbf{m}_1)_i) = (\Phi_{\mathbf{m}_1}(\mathbf{c}_1))_i = (\mathbf{w}_1)_i = (\mathbf{w}_2)_i = (\Phi_{\mathbf{m}_2}(\mathbf{c}_2))_i = \varphi((\mathbf{c}_2)_i, (\mathbf{m}_2)_i).$$

Now, since  $(\mathbf{m}_1)_i = \mathbf{M}_i = (\mathbf{m}_2)_i$  and  $\varphi_{\mathbf{M}_i,2}$  is a bijection, this shows that

$$(\mathbf{c}_1)_{I_X} = (\mathbf{c}_2)_{I_X}.$$

Thus,

$$(\mathbf{c}_1)_I = (\mathbf{c}_2)_I.$$

Now, by Proposition 3, we get that

$$(\mathbf{c}_1)_{Y_1} = (\mathbf{c}_2)_{Y_1}$$

since

$$|C_{Y_1}(I, (\mathbf{c}_1)_{Y_1})| = |A|^{r(Y_1)-r(I)} = 1.$$

This concludes the proof that  $D$  is an almost affine code since:

- for  $i \in Y \cap B \subset Y_1$ ,

$$(\mathbf{w}_1)_i = (\mathbf{c}_1)_i = (\mathbf{c}_2)_i = (\mathbf{w}_2)_i,$$

- for  $i \in Y \cap X \subset Y_1$ ,

$$(\mathbf{w}_1)_i = \varphi((\mathbf{c}_1)_i, (\mathbf{m}_1)_i) = \varphi((\mathbf{c}_1)_i, \mathbf{M}_i) = \varphi((\mathbf{c}_1)_i, (\mathbf{m}_2)_i) = (\mathbf{w}_2)_i,$$

- for  $i \in Y_2$ ,

$$(\mathbf{w}_1)_i = (\mathbf{w}_2)_i$$

by assumption.

But this also shows that the rank function of  $M_D$  is given by

$$r_{D_{X,M}}(Y) = |I \cup Y_2| = r(Y \cap (B \cup X)) + |Y \setminus (B \cup X)|,$$

which in turn shows that this just depends on  $X$ , not on  $\mathbf{M} \in A^X$ .  $\blacksquare$

**Remark 4** For every  $\mathbf{m} \in A^{E \setminus B}$  such that  $(\mathbf{m})_X = \mathbf{M}$ , the code  $C_{\mathbf{m}}$  is an almost affine subcode of  $D_{X,M}$ . They define a pair of codes, whose associated demi-matroid will be denoted  $(E, \rho_X)$ .

#### 4.2.2 Conditional entropy of the system

We want to see how much an intruder gets of information by listening to  $\mu$  digits of the sent message, and knowing already a subset  $X$  of the digits of the message  $\mathbf{m}$ . We will need two lemmas. The first one tells, given that the original message was  $\mathbf{m} \in A^{E \setminus B}$  and that the intruder listens to  $\mathbf{t} \in A^Y$ , how many possible  $\mathbf{w} \in C_{\mathbf{m}}$  might have been sent over the channel. The second one tells how many messages  $\mathbf{m} \in A^{E \setminus B}$  may have possibly be sent, given that  $\mathbf{m}_X = \mathbf{M}$ , and given that the intruder listens to  $\mathbf{t} \in A^Y$ .

**Lemma 6** Let  $\mathbf{M} \in A^X$  and  $Y \subset E$ . Let  $\mathbf{m} \in A^{E \setminus B}$  and  $\mathbf{t} \in A^Y$ . Define

$$\Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m}) = \begin{cases} \emptyset & \text{if } \mathbf{m}_X \neq \mathbf{M}, \\ \{\mathbf{w} \in C_{\mathbf{m}}, \mathbf{w}_Y = \mathbf{t}\} & \text{otherwise} \end{cases}$$

Then  $\Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m})$  is either empty or has cardinality  $|A|^{k-r(Y)}$ .

**Proof** This is essentially the first part of [4, Lemma 9].  $\blacksquare$

**Lemma 7** Let  $\mathbf{M} \in A^X$  and  $\mathbf{w} \in D_{X,\mathbf{M}}$ . Let  $Y \subset E$  and  $\mathbf{t} = \mathbf{w}_Y$ . Then

$$\left| \{ \mathbf{m} \in A^{E \setminus B}, \Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m}) \neq \emptyset \} \right| = |A|^{n-k-|X|-\rho_X(Y)}.$$

**Proof** We compute  $|\{ \mathbf{v} \in D_{X,\mathbf{M}}, \mathbf{v}_Y = \mathbf{t} \}|$  in two different ways. Since  $D_{X,\mathbf{M}}$  is a disjoint union of  $C_{\mathbf{m}}$ , we have

$$\begin{aligned} |\{ \mathbf{v} \in D_{X,\mathbf{M}}, \mathbf{v}_Y = \mathbf{t} \}| &= \sum_{\mathbf{m} \in A^{E \setminus B}, \mathbf{m}_X = \mathbf{M}} |\{ \mathbf{v} \in C_{\mathbf{m}}, \mathbf{v}_Y = \mathbf{t} \}| \\ &= \sum_{\mathbf{m} \in A^{E \setminus B}, \mathbf{m}_X = \mathbf{M}} |\Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m})| \\ &= \sum_{\mathbf{m} \in A^{E \setminus B}, \Omega_{\mathbf{t},x,\mathbf{M}}(\mathbf{m}) \neq \emptyset} |\Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m})| \\ &= \sum_{\mathbf{m} \in A^{E \setminus B}, \Omega_{\mathbf{t},x,\mathbf{M}}(\mathbf{m}) \neq \emptyset} |A|^{k-r(Y)} \\ &= |\{ \mathbf{m} \in A^{E \setminus B}, \Omega_{\mathbf{t},Y,\mathbf{M}}(\mathbf{m}) \neq \emptyset \}| |A|^{k-r(Y)}. \end{aligned}$$

On the other hand, since  $D_{X,\mathbf{M}}$  is an almost affine code, and  $\mathbf{w} \in D_{X,\mathbf{M}}$ , by [9, Proposition 2], we have

$$|\{ \mathbf{v} \in D_{X,\mathbf{M}}, \mathbf{v}_Y = \mathbf{t} \}| = |D_{X,\mathbf{M}}(\mathbf{w}, Y)| = |A|^{r_{D_{X,\mathbf{M}}}(E) - r_{D_{X,\mathbf{M}}}(Y)}.$$

The lemma follows easily.

A way of measuring how much an intruder gains information is the conditional entropy of the system, namely

$$H(\mathbf{m}|\mathbf{t}, \mathbf{M}) = \sum_{\mathbf{M} \in A^X, \mathbf{t} \in A^Y} p(\mathbf{M}, \mathbf{t}) \sum_{\mathbf{m} \in A^{E \setminus B}} p(\mathbf{m}|\mathbf{t}, \mathbf{M}) \log_{|A|} \frac{1}{p(\mathbf{m}|\mathbf{t}, \mathbf{M})},$$

where  $p(\mathbf{M}, \mathbf{t})$  is the probability to get both  $\mathbf{M}$  and  $\mathbf{t}$ , while  $p(\mathbf{m}|\mathbf{t}, \mathbf{M})$  is the probability the probability that  $\mathbf{m}$  is the original message, knowing that  $\mathbf{m}_X = \mathbf{M}$  and that the intruder listens to  $\mathbf{t}$ , and with the convention that  $0 \log_{|A|} \frac{1}{0} = 0$ . The conditional entropy is a measure of how many digits the intruder still does not know on the original message  $\mathbf{m}$ , if he has knowledge of a subset  $X$  of the symbols of  $\mathbf{m}$ , and been able to listen to a subset  $Y$  of the symbols of the message  $\mathbf{w} \in C_{\mathbf{m}}$  sent through the channel. For example, if the intruder is able to listen to everything, then  $p(\mathbf{m}|\mathbf{t}, \mathbf{M})$  is either 0 or 1 (it is 1 if and only if  $\mathbf{m}$  is the original message), so the conditional entropy is 0. On the other hand, if the intruder cannot tap any digit, then  $p(\mathbf{M}, \mathbf{t}) = \frac{1}{|A|^{|X|}}$  and  $p(\mathbf{m}|\mathbf{t}, \mathbf{M})$  is either 0 if  $\mathbf{m}_x \neq \mathbf{M}$  or  $\frac{1}{|A|^{|E \setminus B| - |X|}}$  if  $\mathbf{m}_x = \mathbf{M}$ , so that the conditional entropy is  $n - k - |X|$ , that is the number of digits of the original message (of length  $n - k$ ) that are still unknown ( $|X|$  digits are known already).

**Remark 5** When we say that the intruder knows  $s$  extra digits, this means that he knows the equivalent of  $s$  digits, not necessarily  $s$  actual digits, but that  $s$  degrees of freedom have been removed.

**Theorem 4** Suppose that  $\mathbf{m} \in A^{E \setminus B}$  and  $\mathbf{t} \in C_{\mathbf{m}}$  are chosen randomly and uniformly. Then the conditional entropy of the system is

$$H(\mathbf{m}|\mathbf{t}, \mathbf{M}) = n - k - |X| - \rho_X(Y).$$

**Proof** By Lemma 7, for a given  $\mathbf{M} \in A^X$  and  $\mathbf{t} \in A^Y$ , we have

$$p(\mathbf{m}|\mathbf{t}, \mathbf{M}) = \begin{cases} 0 & \text{if } \Omega_{\mathbf{t}, Y, \mathbf{M}}(\mathbf{m}) = \emptyset \\ \frac{1}{|A|^{n-k-|X|-\rho_X(Y)}} & \text{otherwise} \end{cases}.$$

Thus

$$\begin{aligned} H(\mathbf{m}|\mathbf{t}, \mathbf{M}) &= \sum_{\mathbf{M} \in A^X, \mathbf{t} \in A^Y} p(\mathbf{M}, \mathbf{t}) \sum_{\mathbf{m} \in A^{E \setminus B}} p(\mathbf{m}|\mathbf{t}, \mathbf{M}) \log_{|A|} \frac{1}{p(\mathbf{m}|\mathbf{t}, \mathbf{M})} \\ &= \sum_{\substack{\mathbf{M} \in A^X, \mathbf{t} \in A^Y \\ p(\mathbf{M}, \mathbf{t}) \neq 0}} p(\mathbf{M}, \mathbf{t}) \sum_{\substack{\mathbf{m} \in A^{E \setminus B} \\ \Omega_{\mathbf{t}, Y, \mathbf{M}}(\mathbf{m}) \neq \emptyset}} p(\mathbf{m}|\mathbf{t}, \mathbf{M}) \log_{|A|} \frac{1}{p(\mathbf{m}|\mathbf{t}, \mathbf{M})} \\ &= \sum_{\substack{\mathbf{M} \in A^X, \mathbf{t} \in A^Y \\ p(\mathbf{M}, \mathbf{t}) \neq 0}} p(\mathbf{M}, \mathbf{t}) \sum_{\substack{\mathbf{m} \in A^{E \setminus B} \\ \Omega_{\mathbf{t}, Y, \mathbf{M}}(\mathbf{m}) \neq \emptyset}} \frac{n-k-|X|-\rho_X(Y)}{|A|^{n-k-|X|-\rho_X(Y)}} \\ &= \sum_{\substack{\mathbf{M} \in A^X, \mathbf{t} \in A^Y \\ p(\mathbf{M}, \mathbf{t}) \neq 0}} p(\mathbf{M}, \mathbf{t}) (n-k-|X|-\rho_X(Y)) \\ &= n-k-|X|-\rho_X(Y). \end{aligned}$$

■

#### 4.2.3 Equivocation of the system

We are interested in minimizing the amount of information an intruder may have access to if he gets  $X$  digits of the original message, and is able to listen to  $\mu$  digits of the message sent over the channel, that is we are interested in maximizing the equivocation

$$E_\mu = \min_{|Y|=\mu} H(\mathbf{m}|\mathbf{t}, \mathbf{M}),$$

or equivalently minimizing

$$\Delta_\mu = n-k-E_\mu,$$

the maximum number of digits known to the intruder after listening to  $\mu$  digits over the channel.

In [1], the authors introduce the following profile of demi-matroids:

**Definition 9** Let  $(E, r)$  be a demi-matroid of rank  $l$ , and let  $0 \leq i \leq l$ .

$$\sigma_i = \min\{|X|, r(X) = i\}.$$

**Theorem 5** The uncertainty is given by

$$\Delta_\mu = |X| + j \Leftrightarrow \sigma_j \leq \mu < \sigma_{j+1}$$

for  $0 \leq j \leq n-|X|-k$  and with the convention that  $\sigma_{n-|X|-k+1} = \infty$

**Proof** We have

$$\Delta_\mu = n-k - \min_{|Y|=\mu} H(\mathbf{m}|\mathbf{t}, \mathbf{M}) = |X| + \max_{|Y|=\mu} \rho_X(Y).$$

It is easy to see that

$$\max_{|Y|=\mu} \{\rho_X(Y)\} = j \Rightarrow \mu \geq \sigma_j$$

and that

$$\mu \geq \sigma_j \Rightarrow \max_{|Y|=\mu} \{\rho_X(Y)\} \geq j.$$

Then we get the equivalence

$$\sigma_j \leq \mu < \sigma_{j+1} \Leftrightarrow \max_{|Y|=\mu} \{\rho_X(Y)\} = j.$$

The theorem follows.  $\blacksquare$

**Remark 6** In a remark on p. 1225 of [6] the authors note that in the analogous set-up there, using linear codes, the adversary can obtain at least  $j$  information bits among-the non-tapped ones, if and only if he/she can tap at least  $m_j$  of the encrypted (and transmitted) information bits. In that paper  $m_j$  is the (relative Hamming weight and) demi-matroid invariant

$$m_j = \min\{|X|, \overline{R}(X) = j\}$$

for  $R(Y) = r_1(Y) - r_2(Y)$ , corresponding to a pair  $(C_1, C_2)$  appearing there. But if instead one looks at  $r(Y) = \overline{R}(Y) = r_2^*(Y) - r_1^*(Y)$ , corresponding to the pair of dual codes  $(C_2^\perp, C_1^\perp)$ , then the  $m_j$  described are precisely the

$$\sigma_j = \min\{|X|, r(X) = j\}$$

described in Definition 9 above.

#### 4.2.4 An example

Let  $A = \mathbb{F}_3^2$  and  $\phi : \mathbb{F}_3^{18} \rightarrow A^9$  defined by

$$\phi(x_1, \dots, x_{18}) = ((x_1, x_2), \dots, (x_{17}, x_{18})).$$

Consider the linear code  $L$  over  $\mathbb{F}_3$  with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Consider the folded code  $C = \phi(L)$ . It can be shown that this code is an almost affine code of length 9 and dimension 3 on the alphabet  $A$ . Moreover, its associated matroid is the non-Pappus matroid (see [9, Example 4]). As such, this code is not equivalent to any linear code. The independent sets of  $M_C$  are all subsets of  $E = \{1, \dots, 9\}$  of cardinality at most 3 except

$$\{1, 2, 3\}, \{1, 5, 7\}, \{1, 6, 8\}, \{2, 4, 7\}, \{2, 6, 9\}, \{3, 4, 8\}, \{3, 5, 9\}, \{4, 5, 6\}.$$

We fix a basis  $B = \{7, 8, 9\}$ .

We wish to send a message  $\mathbf{m} \in A^6$ , but an intruder has knowledge of the two last digits of the message (that is,  $X = \{5, 6\}$ ), and is able to listen to  $\mu$  digits of the sent message. How much information does the intruder know about the message  $\mathbf{m}$ . Obviously, the intruder knows at least 2 digits. But the choice of the  $\mu$  digits gives the intruder different amount of information.

The matroid associated to the code  $D_{X,M}$  is a matroid of rank 7 on  $E$ , with the following bases:

$$\begin{aligned} &\{1, 2, 3, 4, 5, 6, 8\}, \{1, 2, 3, 4, 5, 7, 9\}, \{1, 2, 3, 4, 5, 7, 8\}, \\ &\{1, 2, 3, 4, 6, 8, 9\}, \{1, 2, 3, 4, 5, 8, 9\}, \{1, 2, 3, 4, 5, 6, 7\}, \{1, 2, 3, 4, 6, 7, 8\}, \\ &\{1, 2, 3, 4, 5, 6, 9\}, \{1, 2, 3, 4, 6, 7, 9\}, \{1, 2, 3, 4, 7, 8, 9\} \end{aligned}$$

The associated demi-matroid of the system has the following sets of profiles:

$$\sigma_0 = 0, \quad \sigma_1 = 3, \quad \sigma_2 = 5, \quad \sigma_3 = 6, \quad \sigma_4 = 7 .$$

From Theorem 5, we know that no matter the choice of the digits an intruder listens to, if he listens to 0, 1, or 2 digits, the intruder gets no information whatsoever on the sent message (except on the digits he already knows). If he is able to listen at most 4 digits, he gets at most 1 digit of extra information. For example, if the intruder listens to digits 4, 5, 6 of the sent message  $\mathbf{m}$ , he gets one extra digit of information (in this case, the intruder actually knows the 4th digit). If the intruder listens to the digits 3, 4, 8, then he also gets one extra digit of information (in the sense of Remark 5, not an actual extra digit). While if he listens to digits 1, 2, 9, he doesn't get any more information.

## References

- [1] Britz, T., Johnsen, T., Martin, J.A.: Chains, Demi-matroids and Profiles. *IEEE Trans. Inform. Theory*, 60, no. 2, 986–991 (2014)
- [2] Britz, T., Johnsen, T., Mayhew D., Shiromoto K.: Wei-type duality theorems for matroids. *Des. Codes Cryptogr.*, 62, no. 3, 331–341 (2012)
- [3] Gordon, G.: On Brylawski's Generalized Duality. *Math. Comput. Sci.*, 6, no. 2, 135–146 (2012)
- [4] Johnsen, T., Verdure, H.: Generalized Hamming weights for almost affine codes. *IEEE Trans. Inform. Theory*, 63, no. 4, 1941–1953 (2017)
- [5] Liu, Z., Chen, W., Luo, Y.: The relative generalized Hamming weight of linear  $q$ -ary codes and their subcodes, *Des. Codes Cryptogr.*, 48, no. 2, 111–123 (2008).
- [6] Luo, Y., Mitropant, C., Han Vinck, A.J., Chen, K.: Some New Characters on the Wire-Tap Channel of Type II. *IEEE Trans. Inform. Theory*, 51, no. 3, 1222–1227 (2005)
- [7] Oxley, J.G.: *Matroid theory*. Oxford university press, New York (2011)
- [8] Ozarow, L.H., Wyner, A.D.: Wire-Tap Channel II. *Advances in cryptology* (Paris, 1984), 33–50, *Lecture Notes in Comput. Sci.*, 209, Springer, Berlin, (1985)
- [9] Simonis, J., Ashikhmin, A.: Almost Affine Codes. *Des. Codes Cryptogr.*, 14, no. 2, 179–197 (1998)
- [10] Wei, V.K.: Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37, no. 5, 1412–1418 (1991)
- [11] Zhuang, Z., Dai, B., Luo, Y., Han Vinck, A.J.: On the relative profiles of a linear code and a subcode. *Des. Codes Cryptogr.*, 72, no. 2, 219–247 (2014)